NAVAL WAR COLLEGE
NEWPORT, RI

WEAPONS OF MASS DISRUPTION FOR THE OPERATIONAL INFO-WARRIOR

by
Timothy B. Killam
Major, United States Air Force

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: 

12 February 1996

Paper Directed by
CAPT D. Watson, USN
Chairman, Joint Military Operations Department

Prof. Roger W. Barnett
Faculty Advisor

Date

Security Classification This Page

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): WEAPONS OF MASS DISRUPTION FOR THE OPERATIONAL INFO-WARRIOR (UNCLASSIFIED)	
9. Personal Authors: Major Timothy B. Killam, USAF	
10.Type of Report: FINAL	**11. Date of Report:** 12 February 1996
12.Page Count: 23	
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: INFORMATION WARFARE, OPERATIONAL, CYBERWAR, DETERRENCE	

15.Abstract: The technological advances of the information age have the potential for drastically altering contemporary ideas about power and its application. Future conflict and warfare have become inextricably intertwined with the information realm of cyberspace. Information Warfare (IW) is the logical extension of applying new and unconventional technologies to power projection and national defense. However, IW is not merely propaganda, command and control warfare (C2W), nor even simply a force multiplier in the operational toolbox. It is a way to control and attack the enemy's Observation, Orientation, Decision, and Action (OODA) loop. Instead of physically removing his "center of gravity" C2 loop as in C2W and making him deaf, dumb, and blind, IW seeks to manipulate the OODA and the cyberspace in which it exists to make the enemy deaf, dumb, and blind to anything except that which we permit him to hear, say, or see. The Weapons of Mass Disruption (WMDi) provide a new and unique capability to render the enemy's operational forces impotent by short circuiting the OODA loop and controlling the enemy's decisions and hence his courses of action. When combined with traditional military operations in a conventional war or OOTW, the effect can be quick, devastating, and decisive.

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-[redacted] 6461		**20.Office Symbol:** C	

Security Classification of This Page Unclassified

WEAPONS OF MASS DISRUPTION FOR THE OPERATIONAL INFO-WARRIOR

ABSTRACT

The technological advances of the information age have the potential for drastically altering contemporary ideas about power and its application. Future conflict and warfare have become inextricably intertwined with the information realm of cyberspace. Information Warfare (IW) is the logical extension of applying new and unconventional technologies to power projection and national defense. However, IW is not merely propaganda, command and control warfare (C2W), nor even simply a force multiplier in the operational toolbox. It is a way to control and attack the enemy's Observation, Orientation, Decision, and Action (OODA) loop. Instead of physically removing his "center of gravity" C2 loop as in C2W and making him deaf, dumb, and blind, IW seeks to manipulate OODA and the cyberspace in which it exists to make the enemy deaf, dumb, and blind to anything except that which we permit him to hear, say, or see. The Weapons of Mass Disruption (WMDi) provide a new and unique capability to render the enemy's operational forces impotent by short circuiting the OODA loop and controlling the enemy's decisions and hence his courses of action. When combined with traditional military operations in a conventional war or OOTW, the effect can be quick, devastating, and decisive.

TABLE OF CONTENTS

The form of any war--and it is the form which should be of primary interest to professional soldiers--depends upon the technical means of war available.

Giulio Douhet, 1921[1]

INTRODUCTION

The information age is here and the technological advances that brought it about have the potential of challenging and changing contemporary ideas about power and its application. The ideas of conflict and warfare have become inextricably intertwined with the information realm and its environment--cyberspace.

For the military professional, the current idea of Information Warfare (IW) is the logical extension of applying unconventional technologies to power projection and national defense. However, the ideas, concepts, doctrine, and strategic vision of IW are in their infancy. In fact, even though the Joint Chiefs of Staff have identified 16 types of war and 17 types of warfare, they have yet to address and agree upon a definition of exactly what IW is and how it is relevant to national strategy.[2] This paper seeks to propose disruptive weapons of IW at the operational level. Specifically, it will examine IW techniques and concepts for the employment of such weapons and discover how they can best be employed as an offensive capability at the operational level of conflict.

BACKGROUND

In the largest sense, IW is simply the use of information to achieve our national objectives. But it is not about satellites, wires, or even computers, it is about influencing human beings and the decisions they make.[3] This can be anywhere at any time, since all human beings process information to make their decisions.

For the warfighter in the operational environment, the main target is the decisions being made by the enemy commander. As Sun Tzu declares in the *Art of*

War, "What is of supreme importance in war is to attack the enemy's strategy." As we shall see, the potential of IW makes this more feasible, since the basis of the enemy's strategy is the decisions he makes.

CJCS Memorandum of Policy 30, defines "Command and Control Warfare" (C2W) as the way the military conducts Information Warfare. Here C2W is defined as a subset of IW consisting of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction.[4] However, some other techniques available to the info-warrior don't fall into the strict definition of C2W. For example, conventional military deception takes active measures, such as false radio traffic and dummy construction, to provide the enemy with observable phenomena to indirectly influence his strategy. In IW, it is possible to alter what he observes or has observed by disrupting the information on which he bases his decisions.[5] In deception, the enemy must interpret what he observes as real, while in IW, his information is taken to be accurate and hence real. The result is the same, however it is more assured as it does not depend on how the enemy interprets what he observes -- an important distinction.

Thus, the definition of C2W may be too restrictive and could limit the military's ability to take advantage of the unique characteristics of the full range of IW in cyberspace. It is important to note that information is the only resource that can exist simultaneously in more than one place and can move at the speed of light. Therefore, it can transcend the time and space limits of physical force, which is normally associated with military operations.[6] This is an option that the operational warfighter

must have available in today's limited force environment.

To follow Sun Tzu, the attack is against the enemy's strategy and the decisions he is making in pursuit of that strategy. The power of IW is to attack the opponent's strategy and defeat it before his first forces can be deployed or his first shots fired. At the operational level this means a custom-tailored IW attack to manipulate the information on which the enemy commander bases his strategy and decisions prior to or in concert with the conduct of more traditional (destructive) military operations. The objective is to change his concept of reality.

This can be accomplished not with fictional forces, but by making him respond to a "fictive" universe. CNN and the mass media culture today have created a world where major decisions are based on "fictive" information. Although what the public sees on CNN is "true", it is just not the whole, relevant, or contextual truth. This has been termed a "fictive" universe and it is the politically relevant framework in which we are supposed to decide and act.[7]

THE EXPLOITABLE INFORMATION GAP

To change the reality in the mind of the enemy commander requires more than mere propaganda and deception, it requires undermining and disrupting the commander's ability to react to the world through his Observation, Orientation, Decision, Action (OODA) loop.

The goal is to exploit the enemy's critical vulnerability of dependence on information by getting inside his OODA loop via his communication networks. His ability to observe can be attacked by slightly altering data and providing contradictory

information. His objective reasoning can be eliminated by replacing his "known" universe with an alternative reality. His decisions increasingly respond to a "fictive" universe created by friendly forces. Finally, his actions can be paralyzed: they are not based on reality any more because his concept of reality has been changed.

So, instead of physically destroying the enemy's command and control networks, as in C2W, and making him deaf, dumb, and blind, IW seeks to manipulate OODA and the cyberspace in which it exists to make the enemy deaf, dumb, and blind to anything except that which we permit him to hear, say, or see. This gives us control over the enemy's information and can lead to strategic paralysis, since the enemy is unable to conduct operations against us in his "fictive" universe.[8]

A key point in both PSYOPs and deception is that the truth is more powerful than a lie. Applying this to offensive IW as well, the closer to the truth the first disruptions are, the more believable. Hence the enemy commander receives information, but it is a steady diet of slightly altered, truth-based, believable information on which he bases his decisions. Gradually he is moved farther and farther away from reality using a technique such as "stair stepping"[9], until he is operating so completely in his own "fictive" universe that any action he takes is just "chasing ghosts". Clearly what is intended here is asymmetric warfare.

The attempt is to pit the strengths of high tech friendly forces against the enemy's weakness--his ability to decide and act realistically in an altered reality. The enemy commander will receive information that is truth based, but altered, while the "stair stepping" moves him further away from reality. By exploiting characteristics of

the data he receives, his mind can literally be changed for him.

Why is the information so believable? The key lies in the distinction between valid data and accurate data. Valid data is in the correct form. Accurate data is correct for the specific conditions. For example, the sine function varies between -1 and 1. Any answer a computer returns in that range is valid, but it might not be the accurate (correct) answer to your problem. The prudent commander will verify that the data is valid, but to verify its accuracy requires time and effort, both of which may be in short supply in a combat environment.[10]

Thus, a weapon that can give the enemy commander data that he expects to see, and is valid but not accurate, would be the first step in moving him away from reality. Since information is what the intelligent mind derives from data, if the data is valid, it will be taken as accurate in the fog of war. This fact reveals a gap in the information realm and is easily exploitable.

Another gap can be illustrated by the question, "Have you stopped beating your wife yet?" An answer of yes implies you used to beat your wife, while a no answer indicates you are still beating your wife. This question is based on an assumption, and it is the assumption that is more central to the answer than the (yes or no) binary response. Yet, computers and high tech systems are all based on silicon chips that use binary logic to address all problems. The finite world of the binary chip can only store data. It is in the mind of the individual receiving and digesting that data that it becomes useful information. Thus, altering the assumptions in the mind of the enemy commander can have a synergistic effect -- another gap that can be exploited by the

info-warrior.

Here PSYOPS and deception augment the exploitation of this information gap by providing the enemy with assumptions of our choosing. These assumptions, once in the enemy commander's mind, change the meaning of the information he is receiving from his high tech systems--just as in the "beating your wife" question. This change provides access to the enemy's OODA loop and creates the environment for the disruptive activities of IW.

WEAPONS OF MASS DISRUPTION

Since the objective in an IW strike is to disrupt and not destroy, the tools of the trade might be characterized as "weapons of mass disruption" or WMDi. These can include various forms of malicious computer software or code, perception management activities, and flexible deterrent options. Other high tech disruptive weaponry, such as mass spectrum directed energy weapons and surgically precise low power particle beam weaponry cause disruption, but through the destruction of key components in the enemy's high tech systems. This paper's focus is on the purely disruptive actions that are unique with WMDi as defined here.

The term "malicious code" can be broken down into four broad categories: viruses, worms, Trojan horses, and logic bombs or torpedoes.[11] These software weapons offer extraordinary attack potential at a low cost with low risk and will thus be examined in detail.[12] Note that the targets may be hardware, software, firmware, wetware, information, or any combination thereof.[13]

Virus: A computer virus is code designed to be self-replicating, undetectable,

transferable, and has the aim of rendering the computer or some of the data unusable. This means that the virus is not designed to destroy the system in the physical sense, but possibly destroy the information in a system by making the data on which it is based unusable. This is seen as a deliberate attack on a system. Modern viruses may be encrypted, compressed, or polymorphic to reduce the possibility of detection.[14]

Worms: Worms differ from viruses in one subtle way in that they do not require a host, ie. are not parasitic. They don't need to reside on the system they are designed to attack, but can come in through a network.[15] A virus also may enter a system through a network, but what distinguishes a worm is that it never has to actually reach the target system. Worms usually attack access and availability of a system instead of the data. They can deny access to legitimate users by overwhelming the system with their offspring.

Trojan Horse: This is a program that is designed to impersonate a legitimate executable program in a system. It hides in a system and can be attached to an executable program to perform unwanted functions while being run. This can corrupt data or transmit it to another location without the operator's knowledge.[16]

Logic Bomb and Torpedo: A logic bomb is a piece of code hidden in a true executable program. It will transparently wait for a certain condition or a particular event to "activate" and deliberately destroy data or software. A similar idea is a logic torpedo, which is in essence a logic bomb which can be sent through a communication or computer network to a target system, actually hunting it down in cyberspace.[17]

Hybrid CVW: The most powerful WMDi would be one which is a hybrid or

technical combination of two or more of the above types of malicious codes. This could be tailored for a specific system and could even have a degree of artificial intelligence. This "super virus" would clearly be designed as a weapon and can be termed the "computer virus as a weapon" or CVW.[18]

Intelligent Agent: Some people term a program that intelligently searches cyberspace to perform a particular function an intelligent agent, since it can carry out tasks without direct human supervision.[19] Even though it behaves like a virus, it can be considered useful. Consider for example, a helpful agent which you instruct to find the best rates and schedule for an airline flight, book the seats, pay for them, and inform the you of any delays or problems.[20] This may sound great, but consider an intelligent agent that carries a hybrid CVW. This weapon could be put into cyberspace at any point, at any time, perform disrupting actions on a grand scale, cover its tracks, report on its progress and remain persistent throughout cyberspace, mutating itself to avoid detection.[21] It might even create other agents, or "learn" and adapt to unfamiliar target systems as the need arises.[22] While a logic torpedo may be misdirected and hence negated by a complex, "self-healing" distributive network, such a CVW agent could be ideal as it could adapt and "track down" the target in cyberspace.[23]

No such attack could be complete without the addition of PSYOP and deception operations to add to the believability of our "fictive" universe. Thus perception management activities can be used to put questions into the enemy's mind. These questions lead to assumptions that can be exploited in the information gap--such as

the intent and will of friendly forces. Various flexible deterrent options can be used to keep the enemy off-balance and add to the fog of the information war.

Putting all these items together into a blitz of activity in an offensive IW strike requires intense planning and coordination.

WMDi IN OFFENSIVE INFORMATION OPERATIONS

The attack on the mind of the enemy commander through his OODA loop requires offensive IW operations, employing weapons that are tailored to his environment and expectations. These offensive IW operations can be at any time during a conflict, but are undoubtedly most effective in a preemptive strike against his use of information.

Preemptive Counterinformation Strike

To alter the enemy commander's perception and reality at the outset of a conflict, it is necessary to preempt his ability to act. A preemptive strike would be lightning fast using weapons designed to exploit gaps and ambiguities in the information realm and lead him into a "fictive" universe. This can be done quickly and effectively with a sudden blitz of hundreds of small independent offensive actions in cyberspace to get inside the OODA loop and short circuit it into a "fictive" universe. This concerted action will be termed an Offensive Counterinformation (OCI) strike.

An OCI strike can be conducted on the eve of a major operational offensive by enabling and exploiting the information realm of cyberspace through deception, PSYOPs, EW, and Special Technical Operations[24] using WMDi.

In the operational environment, concepts such as surprise and economy of force

carry new weight in a preemptive OCI strike since it is undetectable and uses no fielded forces. The inherent nature of altering the enemy's actions through his OODA loop, gives friendly forces a unique freedom of action to apply the minimum force necessary to force the enemy to our will.

In fact, it is possible to conduct an OCI strike, altering enemy information to the point where the decision the enemy commander makes is not to fight. Or, in the words of Colonel Tanksley, US Army Intelligence and Security Command, "We may be able to stop a war before it starts."[25] This is true deterrence, the "ultimate" in economy of force and lends credence to the argument that IW and WMDi are most effective when employed preemptively.

Considerations For Operational WMDi Employment

Modern warfare in the conventional sense has two main characteristics, speed and lethality. Speed is of the essence in staying inside the enemy's OODA loop since his reality must be altered faster than he can react. Thus, WMDi are uniquely applicable to modern conventional warfare as they can provide the lightening fast actions required.

Lethality is not an area WMDi are tailored for; however, modern warfare while lethal, not only seeks to destroy the enemy forces more efficiently, but also helps to put fewer of our forces at risk through its advanced technology. The pure nature of a preemptive OCI strike would have no forces at risk, while such a strike during a conflict would put no additional forces at risk.

In the OCI strike, the attack is against the enemy plans, strategy, and ability to

make decisions; this is different from direct physical attack. The object is not to destroy, but disrupt his ability to be effective. However, non-lethal IW may have lethal consequences and that fact should be considered.

The effective use of IW techniques at the operational level of warfare can provide advantages to the commander in three specific areas: as an enabler/enhancer of physical force, in direct attacks against enemy will, and against significant enemy information not directly related to the physical conflict.[26]

First, by creating a "fictive" universe in which the enemy decides how to act, his forces can be in the wrong place at the wrong time. This directly enhances the effectiveness of friendly forces. In addition, direct IW attacks on the operational logistics information infrastructure of the enemy to interdict his supply lines could limit the forces and supplies available to the enemy, enabling friendly forces to be more effective.

Secondly, IW and the WMDi offer the ability to conduct operations at several levels. For example, the enemy's center(s) of gravity may be attacked at various levels through the same OCI strike. In a particular situation the operational and tactical center of gravity may be the mind of the enemy commander which is making operational decisions. However, the strategic center of gravity might include the enemy's national will (government will and popular will), alliances, the enemy's economy, industrial-base, and infrastructure.[27] The disorientation of the primary decision-maker may be the decisive point at the operational level, but the ability of IW to have a synergistic effect at the strategic level can ensure victory or preemptive

deterrence depending on the desired end state.

Finally, the desired end state is also important in Operations Other Than War (OOTW), or in terms of IW, Information OOTW or IOOTW. There is much discussion about the use of IW to bring down a nation's banking system, disrupt its civilian communications capabilities, or any number of actions against the infrastructure of a society. This is definitely IW between nations, but the targets are information systems not directly related to the physical conflict. Once again, the distinction is the dimension of non-lethal weapons to disrupt without destroying and this is especially important in post-conflict nation building operations or OOTW where we wish to limit the level of destruction. In fact, if the desired end state is to rebuild a nation, it is important to only disrupt the infrastructure to achieve information superiority and not destroy it during the conflict. This will make the post-conflict nation building potentially cheaper and easier.

The successful execution of an operational level IW strike, whether preemptive to prevent conventional warfare or during the course of a campaign must take into account some unique requirements and circumstances.

Objective: The objective in an OCI strike is to disrupt the enemy's plans for offensive action and impair his response to friendly actions by short circuiting the OODA loop in the mind of the enemy commander. If successful, this would result in his forces being in the wrong place at the wrong time to be effective and totally misreading whatever threat friendly forces present.

Intelligence: The need to target a specific enemy and possibly even an individual

commander in an OCI strike requires a massive amount of intelligence information. Much of this is quickly obtainable through cyber-espionage in cyberspace itself, while other items require traditional Human Intelligence (HUMINT) efforts and long lead time. The use of high tech computer software such as sniffers[28] can be used to great effect in obtaining such information. The intelligence community would thus gain the "keys to the kingdom" and have available all information on the enemy's technical systems which can be exploited.

Weapon design: IW weapons need to be very specifically tailored. More than just system compatibility, the WMDi must be tailored for the specific configuration of the enemy command structure and possibly even an individual decision-maker who is being influenced by other disruptive actions. In addition, some areas of the enemy culture and mind set that we wish to target will require "creations" for PSYOP and deception. These may use the mass media to influence the population, or target a particular niche in society with propaganda. This development will require time and some carefully acquired HUMINT information.

Planning: Considering the number of requirements in intelligence, weapon design, and the specific time-based needs in coordinating the conduct of an OCI strike, the planning process must be very accurate and comprehensive. A successful OCI strike can not be planned in a vacuum, thrown together quickly, or be planned years ahead and sitting on a shelf. Rather, friendly forces must include personnel who are constantly on the cutting edge of the current information technology, know what types of weapons are to be employed, and know the areas of the global network

susceptible to exploitation. At the same time, a large intelligence gathering apparatus is necessary and must be closely coordinated with the operational environment to shorten the lead time necessary as a crisis develops.

Conduct: In conducting an OCI strike, it is important to coordinate, integrate, deconflict, and synchronize the massive blitz of PSYOP, deception, and proactive IW operational and tactical activities that characterize the strike, to ensure success. While this is the case in IW operations during a campaign as well, it is of most importance for a preemptive strike. The focus is to flood the enemy sensors with conflicting data and wear out their capability to discern true information. Intelligence will provide insight into what "back-up systems" and independent means of verifying data the enemy has. These too must be targeted and exploited to access how effective the strike is in creating the "fictive" universe and how well the enemy commander is reacting within it.

Effectiveness: To determine the effectiveness of the OCI strike, the following questions must be considered:

-- Does the enemy have other independent sources of information to verify the information of the "fictive" universe created for him? Of greatest concern are low tech sources of information or sources friendly to allies that can not be targeted.

-- Does the plan rely too much on one component of the IW OCI blitz? The intended effect is synergistic, so every element is important, but not at the expense of other efforts. This requires coordination and indepth planning.

-- Is the enemy's reality being altered faster than he can react? This is what

it means to be inside his OODA loop. In the ideal situation the enemy may not even know he is being attacked.

-- Has the primary decision-maker been correctly identified? Is he the focus of the disruptive actions to produce a "fictive" universe? Does the enemy have distributed control of his forces? The effectiveness of the OCI blitz depends on precise targeting for the unique enemy situation.

-- Has the "stair stepping" required to gradually move him farther and farther from reality and into the "fictive" universe been precisely timed and coordinated?

-- How will Information Damage Assessment (IDA) be conducted? This is of the utmost importance in determining the effectiveness of the OCI blitz. The "stair stepping" of the enemy OODA loop requires IDA to evaluate "which way" the enemy's decisions are "moving". Efforts must be made to accurately determine how he is reacting within the "fictive" universe.

-- In the conduct of operations, will a good source of friendly intelligence be removed or disrupted? The source might need to be depended on for this or future operations. Coordination and in depth planning are again all important.

-- What about collateral damage and unintended consequences? For example, even if IW is non-lethal, disrupting air control radars may cause some aircraft, including commercial, to crash. Also, consider the possibility of fratricide to friendly systems. Since they are connected to the target system in cyberspace, a virus weapon or logic torpedo may infiltrate a friendly system by accident.

CONCLUSIONS

The information age and the global network in cyberspace are realities. IW will undoubtedly be a major component of any future conflict whether at the strategic or operational level. It is vitally important that the United States has the ability to conduct IW operations; not only to protect ourselves, but to conduct offensive operations that can bend an enemy to our will without the massive destruction and loss of life as in the conflicts of previous generations. In this sense, the ability to conduct IW operations may provide a strong deterrent to other technologically advanced nations. However, third world, low tech countries may not be deterred by something that would have little direct effect on them.

In the post-Cold War era of reduced defense spending and limited resources, offensive IW and the associated weapons of mass disruption can provide a low-cost and low-risk alternative to massive military intervention. General Colin Powell summarized the essence of the situation: "A downsized force and a shrinking defense budget result in an increased reliance on technology, which must provide the force multiplier required to ensure a viable military deterrent."[29] The instantaneous response and devastating effects of WMDi provide a powerful and credible deterrent.

The ability to exploit the inherent weaknesses in the information gap and alter the decisions the enemy commander is making can lead him to the point where the effectiveness of his forces are extremely limited. For the operational info-warrior, when WMDi are combined with traditional military operations either in a conventional war or OOTW, the effect can be quick, devastating, and decisive.

ENDNOTES

1. Barry Watts, The Foundations of US Air Doctrine: The Problem of Friction in War, (Maxwell AFB, AL: Air University Press, 1984), 6.

2. Wyatt Cook, "Information Warfare: A New Dimension in the Application of Air and Space Power", (Maxwell AFB, AL: Air University Press, 1994), 9.

3. George J. Stein, "Information Warfare", Airpower Journal, Spring 1995, 32.

4. U.S. Joint Chiefs of Staff (Chairman), Command and Control Warfare, Memorandum of Policy No. 30, 1st Revision (CJCS MOP 30), (Washington, DC: 8 March 1993), 3.

5. U.S. Air Force, Cornerstones of Information Warfare, (Washington DC: 1994), 7.

6. Mark Tempestilli, "Waging Information Warfare: Making the Connection Between Information and Power in a Transformed World", Unpublished Research paper, US Naval War College, Newport, RI: June 1995, 6.

7. Stein, 34.

8. Ibid, 37.

9. "Stair stepping" can be defined as a technique to make minor alterations in the data, the observables in the OODA loop, causing the enemy commander's decisions to be "incorrect" for the "true" data, leading to inappropriate actions. The next change in the data builds on this disruption, moving the enemy commander's mind and hence his decisions further afield in the same direction.

10. As a numerical analyst and software designer, in my experience testing numerical software, it is vital to determine if the software has addressed all conditions and whether the answer is merely valid or indeed accurate. As a combat crew commander deployed in Desert Storm, I was always mindful of just how believable the numbers on the computer screen were. However, in the fog of war, there isn't time to error check.

11. Paul Evancoe and Mark Bentley, "CVW--Computer Virus as a Weapon", Military Technology, May 1994, 39.

12. Tempestilli, 14.

13. Firmware is defined as programmable hardware and wetware is a contemporary term for the human brain.

14. Julie Ryan and Gary Federici, "Offensive Information Warfare--A Concept Exploration", (Center for Naval Analyses, VA), July 1994, 5. A polymorphic virus is one that mutates and changes its "shape" as it reproduces in order to avoid detection.

15. Evancoe and Bentley, 39.

16. Ibid.

17. Ryan and Federici, 5.

18. Evancoe and Bentley, 40.

19. Tempestilli, 14.

20. Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway, (New York: Thunder's Mouth Press, 1994), 108.

21. Evancoe and Bentley, 40.

22. Tempestilli, 14.

23. Ibid, 15.

24. Joint Chiefs of Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, Research Report, (Washington, DC: July 1995), A-32.

25. Douglas Waller, "Onward Cyber Soldiers", Time, 21 August 1995, 39.

26. Tempestilli, 18.

27. Cook, 16.

28. Sniffers can be defined as small reconnaissance pieces of software that go through cyberspace to a target system and linger, recording information such as passwords and user accounts. This information would then be reported back to the originator.

29. Colin L. Powell, "Information-Age Warrior", Byte, July 1992, 370.

BIBLIOGRAPHY

Arquilla, John. Cyberwar Is Coming!. Santa Monica, CA: Rand, 1992.

Cook, Wyatt C. Information Warfare: a New Dimension in the Application of Air and Space Power. Maxwell AFB, AL: Air University Press, 1994.

Denning, Peter J., ed. Computers Under Attack: Intruders, Worms, and Viruses. New York: ACM Press, 1990.

Dishong, Donald J. On Studying the Effect of Information Warfare on C2 Decision Making. Monterey, CA: Naval Postgrad School, 1994.

Eisen, Stefan, Jr. "Netwar: It's not just for Hackers Anymore". Unpublished Research Paper, US Naval War College, Newport, RI: June 1995.

Evancoe, Paul R. and Mark Bentley. "Computer Viruses Loom as Future Era Weapons". National Defense, February 1994: 19-21.

Evancoe, Paul R. and Mark Bentley. "CVW--Computer Virus as a Weapon". Military Technology, May 1994: 38-40.

Giboney, Thomas B. "Commander's Control from Information Chaos". Military Review, November 1991, 34-38.

Matthews, William. "Girding for Cyberwar: Information Blitz Could Be Key in Future Battles". Air Force Times, 18 July 1994, 36.

Powell, Colin L. "Information-Age Warriors". Byte, July 1992, 370.

Ryan, Julie, and Gary Federici. "Offensive Information Warfare--A Concept Exploration". Center for Naval Analyses, VA, July 1994.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.

Stein, George J. "Information Warfare". Airpower Journal, Spring 1995, 30-39.

Szafranski, Col Richard. "A Theory of Information Warfare: Preparing for 2020". Airpower Journal, Spring 1995, 56-65.

Tempestilli, Mark. "Waging Information Warfare: Making the Connection Between Information and Power in a Transformed World". Unpublished Research Paper, US Naval War College,

Newport, RI: June 1995.

Toffler, Alvin. The Third Wave. New York: William Morrow and Company, Inc., 1980.

Toffler, Alvin and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. Boston: Little, Brown and Co., 1993.

U.S. Air Force. Cornerstones of Information Warfare. Washington, DC: 1994.

U.S. Army Training and Doctrine Command. Information Operations. Draft FM 100-6, Ft Monroe, VA: 22 Jul 94.

U.S. Joint Chiefs of Staff. Joint Command and Control Warfare (C2W) Operations. Joint Publication 3-13, Second Draft. Washington, DC: 15 January 1994.

U.S. Joint Chiefs of Staff. Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance. Research Report. Washington, DC: July 1995.

U.S. Joint Chiefs of Staff (Chairman). Command and Control Warfare. Memorandum of Policy No. 30, 1st Revision (CJCS MOP 30). Washington, DC: 8 March 1993.

Waller, Douglas. "Onward Cyber Soldiers". Time, 21 August 1995, 38-46.

Watts, Barry. The Foundations of US Air Doctrine: The Problem of Friction in War. Maxwell AFB, AL: Air University Press, 1984.